IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: :
                                          : Group Art Unit: 3621
    Nicholas Sauriol et al.   :
                                          : Examiner: P. Elisca
Appln. No.: 09/749,408   :
                                          : Conf. No.: 5257
Filed: December 28, 2000   :
                                          :
For: SECURE DATABASE FOR   :
     E-COMMERCE   :

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

TABLE OF CONTENTS

I.   INTRODUCTION

In response to the Office Action dated September 6, 2006, finally rejecting pending claims 1-12, Appellant respectfully requests that the Board of Patent Appeals and Interferences reconsider and withdraw the rejections of record, and allow the pending claims, which are attached hereto as an Appendix A.

II.   REAL PARTY IN INTEREST

The real party in interest is Nortel Networks Limited, the assignee of the above-referenced application.

III. RELATED APPEALS AND INTERFERENCES

There are no known related appeals or interferences.

IV.   STATUS OF CLAIMS

Claims 1-12 are pending in this application.   The rejection of claims 1-12 is appealed.

V.   STATUS OF AMENDMENTS

No amendments to the claims have been filed subsequent to the final rejection dated September 6, 2006.

VI.   SUMMARY OF CLAIMED SUBJECT MATTER

Appellant believes that a brief discussion of the background technology, followed by a brief summary of the embodiments of the invention and the problems solved by the embodiments of the present invention, will assist the Board of Patent Appeals and Interferences (hereinafter referred to as

"the Board") in appreciating the significant advances made by the embodiments of the present invention. Finally, concise explanations of each of the independent claims is provided, including reference to exemplary portions of the specification and figures.

A. The Background

The growth of the Internet and other interconnected processor based networks has made it more convenient than ever to conduct E-commerce transactions. E-commerce may comprise the use of computers and electronic communications in business transactions. For example, E-commerce may include the use of electronic data interchange (EDI), electronic money exchange, Internet advertising, websites, online databases, computer networks, and point-of-sale (POS) computer systems.

One drawback of existing E-commerce systems is that when a consumer makes a purchase on-line (i.e., over the network, or on the Internet), most often it is over an unsecured line. As its name suggests, an unsecured line is susceptible to tampering, interception and other fraudulent activities.

Both vendors and consumers are vulnerable to fraud when transacting E-commerce over an unsecured line. For example, vendors may suffer penalties and other fees from credit providers (e.g., Visa.TM., MasterCard.TM., American Express.TM.,

etc.) for cancelled orders due to fraudulent charges. Likewise, consumers face credit history issues, liability for charges, and other unpleasant problems due to theft of their credit information.

Even the use of a secured line can have drawbacks. For example, many Internet sites are set up to prevent unauthorized people from seeing the information that is sent to or from those sites. These are called "secured" sites and may offer the customer some level of protection for their financial information. However, even with a secured line, vendors are still susceptible to fraud. For example, credit card numbers previously stolen from elsewhere may be used on a secure site. Likewise, computer programs exist that will generate fraudulent credit card numbers that will pass through some authorization checks (e.g., the card digits will satisfy a checksum authorization, etc.). Thus, the vendor is still exposed to fraudulent behavior even if the site is secured.

Another drawback of secured sites is that some secured sites require a higher level of connection security than what typically is installed on a consumer's computer. For example, in the United States or Canada, consumers may use 128-bit secured connection support, however, due to legal restrictions this software is not available worldwide.

In view of the foregoing, it would be desirable to provide a technique for conducting E-commerce which overcomes the above-described inadequacies and shortcomings. More particularly, it would be desirable to provide a technique for providing a database which maintains customer financial information in a secure fashion to enable customers and merchants (collectively, "users") to make E-commerce transactions in an efficient and cost effective manner.

B.   Explanation of Independent Claim 1

A method for enabling E-commerce transactions between a vendor and a consumer using a secured network having a host with stored consumer data and approved vendor information, the method comprising the steps of:

enabling the consumer to initiate an E-commerce transaction with the vendor;

enabling the vendor to transmit transaction information related to the E-commerce transaction to the host;

receiving transaction information from the vendor at the host;

processing the transaction information at the host to determine whether the transaction information conforms with the stored consumer data and approved vendor information; and

delivering to the vendor, via the secured network, the

-4-

stored consumer data if the transaction information is determined to conform with the stored consumer data and approved vendor information wherein receipt of the stored consumer data by the vendor enables the vendor to receive payment for the E-commerce transaction.

C. **Explanation of Independent Claim 5**

An apparatus for enabling E-commerce transactions between a vendor and a consumer, the apparatus comprising:

a transaction receiver that receives transaction information from the vendor over the secured network;

a processor that processes the transaction information to determine whether the transaction information conforms with the stored consumer data and approved vendor information; and

a delivery module that delivers to the vendor the stored consumer data if the transaction information is determined to conform with the stored consumer data and approved vendor information, wherein receipt of the stored consumer data by the vendor enables the vendor to receive payment for the E-commerce transaction.

VII. **GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL**

The issues on appeal are whether the following rejections are proper: (1) the rejection under 35 U.S.C. § 103(a) of claims 1, 3, 4, 5, 7 and 8-12 based on Foster (U.S. Patent No.

6,332,134) in view in view of Segal (U.S. Patent No. 6,820,804), and (2) the rejection under 35 U.S.C. § 103(a) of claims 2 and 6 based on Foster (U.S. Patent No. 6,332,134) in view in view of Weber (U.S. Patent No. 6,178,409).

VIII.   ARGUMENT

A.   The Rejection Under 35 U.S.C. § 103(a) of claims 1, 3, 4, 5, 7 and 8-12 based on Foster in view of Segal is Improper

Claims 1, 3, 4, 5, 7 and 8-12 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Foster in view of Segal (6,820,804). This rejection is hereby respectfully traversed.

The Examiner alleges that Foster discloses "delivering to the vendor, via the secured network, the stored consumer data if the transaction information is determined to conform with the stored consumer data and approved vendor information." Office Action, Pages 2-3. The Applicant respectfully disagrees. Foster does not disclose or suggest "delivering to the vendor, via the secured network, the stored consumer data."

Instead, Foster discloses the use of "[m]ultiple user identifiers (Ids) and passwords [which] can be assigned to different people to obtain credit from the same credit card" (Col. 2, lines 41-43.) Clearly, Foster teaches away from secured networks. See, e.g., "The secure electronic (SET)

protocol, while having promise, has been abandoned by key players in the industry. At this point in time, secure socket layer (SSL) is in the fall back position, particularly on the Internet." (Col. 2, lines 2-6). In fact, Foster also teaches minimizing the amount of consumer data that is transmitted. See, e.g. Col. 2, lines 32-40. Thus, Foster discloses the use of Ids and passwords and the minimizing of transmitting data. Therefore, Foster does not disclose or suggest the limitations in claim 1 of "delivering to the vendor, <u>via the secured network</u>, the stored consumer data." For the same reasons, Foster also does not disclose or suggest the limitations of "receiv[ing] transaction information from the vendor <u>over the secured network</u>" as recited in independent claim 5.

Segal does not disclose or suggest sending transaction information or stored consumer data over a "secured network." Segal is directed at a method for "performing purchase transactions .. [using] a home entertainment device (HE) having a display screen" (Segal, abstract). As such, Segal fails to remedy the above noted deficiencies of Foster.

Additionally, the Examiner acknowledges that Foster fails to disclose that "receipt of the stored consumer data by the vendor enables the vendor to receive payment for the e-commerce transaction." Office Action, page 3. The Examiner relies on

Segal to allegedly disclose this feature. Applicant respectfully submits that Segal, as cited by the Examiner, does not disclose or suggest "delivering to the vendor, <u>via the secured network</u>, the <u>stored consumer data</u> if the transaction information is determined to conform with the <u>stored consumer data</u> and approved vendor information wherein receipt of the <u>stored consumer data</u> by the vendor enables the vendor to receive payment for the E-commerce transaction." Segal discloses the user transmitting any required data to the vendor and not the use of the "secured network" for the "receipt of <u>stored</u> consumer data" from "a <u>host</u> with stored consumer data and approved vendor information." Segal discloses the consumer providing any required data to the merchant for each transaction via their home entertainment device. *See, e.g.,* col. 2, lines 28-34. Clearly, Segal does not disclose a "secured network having a host" transmitting "stored consumer data" to the vendor, the receipt of which enables the vendor to receive payment.

Foster, as noted above, does not disclose "receipt of the stored consumer data" over a "secure network." On the contrary, Foster discloses "[i]nstead of cardholders transmitting their card numbers to merchants, the system obtains merchant information and requests the cardholders own card company pay the merchant." (Col 2, lines 32-35). Thus, the proposed

-8-

combination of Foster and Segal does not disclose or suggest either transactions via a "secured network" or a host transmitting data to a vendor wherein the "receipt of stored consumer data by the vendor enables the vendor to receive payment for the E-commerce transaction."

The Office Action has failed to set forth a *prima facie* case of obviousness for the claims. Specifically, when a primary reference is missing elements, the law of obviousness requires that the Office set forth some motivation why one of ordinary skill in the art would have been motivated to modify the primary reference in the exact manner proposed. *Ruiz v. A.B. Chance Co.*, 234 F.3d 654, 664 (Fed. Cir. 2000). In other words, there must be some recognition that the primary reference has a problem and that the proposed modification will solve that exact problem. All of this motivation must come from the teachings of the prior art to avoid impermissible hindsight looking back at the time of the invention.

The mere fact that Foster can be modified does not render the resultant modification obvious unless there is a suggestion or motivation found somewhere in the prior art regarding the desirability of the combination or modification. *See* M.P.E.P § 2143.01; *see also In re Mills*, 16 U.S.P.Q.2d 1430, 1432 (Fed. Cir. 1990); *In re Fritz*, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992).

In addition, the teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in Applicants' disclosure. *In re Vaeck*, 947 F.2d 488, 20 U.S.P.Q.2d 1438 (Fed. Cir. 1991).

In *In re Hedges*, 783, F.2d 1038, 1041, 228 U.S.P.Q. 685, 687, (Fed. Cir. 1986), the U.S. Court of Appeals for the Federal Circuit stated that "the prior art as a whole must be considered. The teachings are to be viewed as they would have been viewed by one of ordinary skill." The court also stated that "'[i]t is impermissible within the framework of section 103 to pick and choose from any one reference only so much of it as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one of ordinary skill in the art'" (quoting *In re Wesslau*, 353 F.2d 238, 241, 147 U.S.P.Q. 391, 393 (CCPA, 1965)). Accordingly, the Office has failed to provide any proper motivation for modifying Foster, so the proposed modification fails. Even if Foster could be modified as suggested by the Office Action, the resulting combination would nevertheless fail to show each and every limitation claimed by Applicants.

Applicants respectfully request that the rejections of claims 1, 3, 4, 5, 7 and 8-12 be withdrawn.

B.   The Rejection Under 35 U.S.C. § 103(a) of claims 2 and 6 based on Foster in view of Weber is Improper

Claims 2 and 6 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Foster in view of Weber, et al. ("Weber"). This rejection is hereby respectfully traversed.

The Examiner admits that Foster does not explicitly disclose the use of a VPN. (Office Action, Page 4). As discussed above, Foster does not disclose or suggest "delivering to the vendor, via the secured network, the stored consumer data" as recited in independent claim 1 or a "transaction receiver that receives transaction information over the secured network" as recited in claim 5. Claims 2 and 6 depend from claims 1 and 5 respectively. As discussed above, Segal fails to cure these deficiencies. The Examiner cites Weber Col. 91, lines 50-61 to allege that Weber discloses a VPN as disclosed by the applicant. Weber discloses a "virtual, private network between the Gateway and the host processor," Col. 91, lines 50-51, and the "HTTPS protocol ..is utilized between the merchants and the Gateway." Col. 92, lines 7-8. See also, "The payment gateway implements secure transactions using RSA public-key cryptography." (Col. 15, lines 32-33). As cited by the Examiner, Weber discloses the use of a VPN only within a corporate gateway to a corporate host. Thus Foster, as discussed above, teaches away from secure networks and Weber

-11-

discloses the use of encryption and not VPNs between a third party's gateway and a merchant. Clearly Weber does not disclose or suggest the use of VPNs between a host and a vendor.

Under 35 U.S.C. § 103, the Patent Office bears the burden of establishing a prima facie case of obviousness. In re Fine, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988). The Patent Office can satisfy this burden only by showing some objective teaching in the prior art or that knowledge generally available to one of ordinary skill in the art would lead that individual to combine the relevant teachings of references. Id. Obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching or suggestion supporting the combination. ACS Hospital Systems, Inc. v. Montefiore Hospital, 732 F.2d 1572, 1577, 221 USPQ 929, 933 (Fed. Cir. 1984). That is, under 35 U.S.C. § 103, teachings of references can be combined only if there is some suggestion or motivation to do so. Id. However, the motivation cannot come from the applicant's invention itself. In re Oetiker, 977 F.2d 1443, 1447, 24 USPQ2d 1443, 1446 (Fed. Cir. 1992). Rather, there must be some reason, suggestion, or motivation found in the prior art whereby a person of ordinary skill in the art would make the combination. Id.

As stated in MPEP § 2143, to establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in applicant's disclosure. In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). Also, as stated in MPEP § 2143.01, obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988); In re Jones, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. In re Mills, 916 F.2d 680, 16 USPQ2d 1430 (Fed.

Cir. 1990). Further, as stated in MPEP § 2143.03, to establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. In re Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). That is, "[a]ll words in a claim must be considered in judging the patentability of that claim against the prior art." In re Wilson, 424 F.2d 1382, 165 USPQ 494, 496 (CCPA 1970). Additionally, as stated in MPEP § 2141.02, a prior art reference must be considered in its entirety, i.e., as a whole, including portions that would lead away from the claimed invention. W.L. Gore & Associates, Inc. v. Garlock, Inc., 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983), cert. denied, 469 U.S. 851 (1984). Finally, if an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious. In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988).

The Examiner relies on Weber to disclose a "virtual private network (VPN) that enables secured communication of the transaction information" and, as such, Weber fails to cure the above noted deficiencies of Foster with respect to claims 1 and 5. Therefore, the combination of Foster and Weber also fails to disclose each feature recited in claims 2 and 6. Applicants respectfully submit that the rejections are improper for at least this reason. In view of the foregoing, it is respectfully

requested that the aforementioned obviousness rejection of claims 2 and 6 be withdrawn.
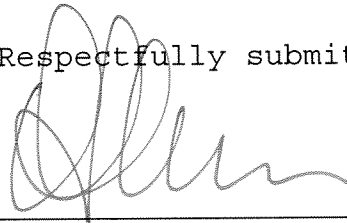
IX. CONCLUSION

In view of the foregoing, it is respectfully submitted that the present application is in condition for allowance, and an early indication of the same is courteously solicited.

To the extent necessary, a petition for an extension of time under 37 CFR § 1.136 is hereby made.

Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 50-0206, and please credit any excess fees to the same deposit account.

Respectfully submitted,

February 6, 2007

Ozzie A. Farres
Registration No. 43,606

Hunton & Williams, LLP
1900 K. St., NW, Suite 1200
Washington, D.C.   20006-1109
Tel. (202) 955-1894
Fax (202) 778-2201

APPENDIX A - CLAIMS

1 (Previously presented).   A method for enabling E-commerce transactions between a vendor and a consumer using a secured network having a host with stored consumer data and approved vendor information, the method comprising the steps of:

enabling the consumer to initiate an E-commerce transaction with the vendor;

enabling the vendor to transmit transaction information related to the E-commerce transaction to the host;

receiving transaction information from the vendor at the host;

processing the transaction information at the host to determine whether the transaction information conforms with the stored consumer data and approved vendor information; and

delivering to the vendor, via the secured network, the stored consumer data if the transaction information is determined to conform with the stored consumer data and approved vendor information wherein receipt of the stored consumer data by the vendor enables the vendor to receive payment for the E-commerce transaction.

2 (Original). The method of claim 1, wherein the step of

providing a secured network further comprises:

provide a virtual private network (VPN) that enables secured communication of the transaction information.

3 (Original). The method of claim 1, wherein the step of processing the transaction information to determine whether the transaction information conforms with the stored consumer data and approved vendor information further comprises:

determining whether the transaction information contains a consumer identification indicator; and

determining whether the transaction information contains a vendor identification indicator.

4 (Previously Presented). The method of claim 3, further comprising:

determining whether the consumer identification indicator conforms with the stored consumer data; and

determining whether the vendor identification indicator conforms with the approved vendor information.

5 (Previously Presented). An apparatus for enabling E-commerce transactions between a vendor and a consumer, the apparatus comprising:

a transaction receiver that receives transaction information from the vendor over the secured network;

a processor that processes the transaction information to determine whether the transaction information conforms with the stored consumer data and approved vendor information; and

a delivery module that delivers to the vendor the stored consumer data if the transaction information is determined to conform with the stored consumer data and approved vendor information, wherein receipt of the stored consumer data by the vendor enables the vendor to receive payment for the E-commerce transaction.

6 (Original). The apparatus of claim 5, wherein the secured network further comprises:

a virtual private network (VPN) that enables secured communication of the transaction information.

7 (Original). The apparatus of claim 5, wherein the processor further comprises:

a consumer identification module that determines whether the transaction information contains a consumer identification indicator; and

a vendor identification module that determines whether the

transaction information contains a vendor identification indicator.

8 (Previously Presented). The apparatus of claim 7, wherein the consumer identification module further comprises a first conformity module that determines whether the consumer identification indicator conforms with the stored consumer data, and wherein the vendor identification module further comprises a second conformity module that determines whether the vendor identification indicator conforms with the approved vendor information.

9 (Previously Presented). The method of claim 1, wherein the transaction information comprises one or more of consumer information, vendor information, transaction amount, and delivery type.

10 (Previously Presented). The method of claim 1, wherein the stored consumer data comprises one or more of credit card account numbers, bank account numbers, consumer name, consumer address, preferred delivery address, preferred billing address, and preferred delivery type.

11 (Previously Presented).   The apparatus of claim 5, wherein the transaction information comprises one or more of consumer information, vendor information, transaction amount, and delivery type.

12 (Previously Presented).   The apparatus of claim 5, wherein the stored consumer data comprises one or more of credit card account numbers, bank account numbers, consumer name, consumer address, preferred delivery address, preferred billing address, and preferred delivery type.

APPENDIX B - EVIDENCE

NONE

APPENDIX C - RELATED PROCEEDINGS

NONE